

# THE ZASSENHAUS FILTRATION, MASSEY PRODUCTS, AND REPRESENTATIONS OF PROFINITE GROUPS

IDO EFRAIT

**ABSTRACT.** We consider the  $p$ -Zassenhaus filtration  $(G_n)$  of a profinite group  $G$ . Suppose that  $G = S/N$  for a free profinite group  $S$  and a normal subgroup  $N$  of  $S$  contained in  $S_n$ . Under a cohomological assumption on the  $n$ -fold Massey products (which holds, e.g., if  $G$  has  $p$ -cohomological dimension  $\leq 1$ ), we prove that  $G_{n+1}$  is the intersection of all kernels of upper-triangular unipotent  $(n+1)$ -dimensional representations of  $G$  over  $\mathbb{F}_p$ . This extends earlier results by Mináč, Spira, and the author on the structure of absolute Galois groups of fields.

## 1. INTRODUCTION

Let  $p$  be a fixed prime number. The  **$p$ -Zassenhaus filtration** of a profinite group  $G$  is the fastest descending sequence of closed subgroups  $G_n$ ,  $n = 1, 2, \dots$ , of  $G$  such that  $G_1 = G$ ,  $G_i^p \leq G_{ip}$ , and  $[G_i, G_j] \leq G_{i+j}$  for  $i, j \geq 1$ . Thus  $G_n = G_{[n/p]}^p \prod_{i+j=n} [G_i, G_j]$  for  $n \geq 2$ . Here given closed subgroups  $H, K$  of  $G$ , we write  $[H, K]$  (resp.,  $H^p$ ) for the closed subgroup generated by all commutators  $[\sigma, \tau]$  (resp.,  $p$ -th powers  $\sigma^p$ ), with  $\sigma \in H$ ,  $\tau \in K$ . This filtration has been studied since the middle of the 20th century both from the group-algebra and Lie algebra viewpoints ([Jen41], [Laz65], [Zas39], [DDMS, Ch. 11–12]), and had important Galois-theoretic applications, e.g., to the Golod–Šafarevič problem [Koc02, §7.7], mild groups, and Galois groups of restricted ramification ([Lab06], [LM11], [Mor04], [Vog05]).

In this paper we interpret the  $p$ -Zassenhaus filtration from the viewpoint of linear representations over  $\mathbb{F}_p$ , and use this to explain and generalize several known facts on the structure of absolute Galois groups of fields. Our first main result characterizes the filtration for free pro- $p$  groups:

---

2010 *Mathematics Subject Classification.* Primary 12G05; Secondary 12F10, 12E30.

*Key words and phrases.* Zassenhaus filtration, Massey products, upper-triangular unipotent representations, profinite groups, absolute Galois groups, Galois cohomology.

This work was supported by the Israel Science Foundation (grant No. 23/09).

**Theorem A.** *Let  $\bar{S}$  be a free pro- $p$  group and  $n \geq 1$ . Then  $\bar{S}_n$  is the intersection of all kernels of linear representations  $\rho: \bar{S} \rightarrow \mathrm{GL}_n(\mathbb{F}_p)$ .*

We may clearly replace here  $\mathrm{GL}_n(\mathbb{F}_p)$  by its  $p$ -Sylow subgroup  $U_n(\mathbb{F}_p)$ , consisting of all upper-triangular  $n \times n$  unipotent matrices over  $\mathbb{F}_p$ . In this reformulation, Theorem A extends to general profinite groups  $G$ , whose defining relations lie sufficiently high in the  $p$ -Zassenhaus filtration, and which satisfy a certain cohomological condition, to be explained below.

Specifically, let  $n \geq 2$ , and suppose that  $G$  can be presented as  $S/N$  for a free profinite group  $S$  and a closed normal subgroup  $N$  of  $S$  contained in  $S_n$  (this can be slightly relaxed - see Remark 11.3). The cohomological condition we assume is on the  $n$ -fold Massey products in the mod- $p$  profinite cohomology ring  $H^\bullet(G/G_n) = H^\bullet(G/G_n, \mathbb{Z}/p)$ . These are maps  $H^1(G/G_n)^n \rightarrow H^2(G/G_n)$ , that generalize the usual cup product (which is essentially the case  $n = 2$ ). According to their general construction (recalled in §3), the Massey products are multi-valued maps. Yet, it was shown by Vogel [Vog05] that in our situation they are well-defined maps (see §8). Moreover, they are multi-linear. Let  $H^2(G/G_n)_{n\text{-Massey}}$  be the subgroup of  $H^2(G/G_n)$  generated by the image of this map. We say that  $G$  satisfies the  **$n$ -th Massey kernel condition** if the kernel of the inflation map  $\mathrm{inf}: H^2(G/G_n)_{n\text{-Massey}} \rightarrow H^2(G)$  is generated by  $n$ -fold Massey products from  $H^1(G/G_n)^n$ . When  $n = 1$  we declare the condition to be true by definition. We prove:

**Theorem A'.** *If  $G$  satisfies the  $n$ -th Massey kernel condition, then  $G_{n+1}$  is the intersection of all kernels of representations  $G \rightarrow U_{n+1}(\mathbb{F}_p)$ .*

The assumptions of Theorem A' are satisfied when  $G$  has  $p$ -cohomological dimension  $\leq 1$  (Corollary 11.4). Hence Theorem A is a special case of Theorem A'.

Theorem A' is elementary for  $n = 1$ . For  $n = 2$ ,  $p = 2$  it was proved in [EM11a], generalizing a result of Mináč and Spira [MSp96] (see also [NQD12]). For  $n = 2$ ,  $p > 2$  it was proved in [EM11b, Example 9.5(1)]. Moreover, it has the following remarkable Galois-theoretic application (§12): Assume that  $G = G_K$  is the absolute Galois group of a field  $K$  containing a root of unity of order  $p$ . Then  $G_3$  is the intersection of all normal open subgroups  $M$  of  $G$  such that  $G/M$  embeds in  $U_3(\mathbb{F}_p)$ . The proof of this fact uses the Merkurjev–Suslin theorem [MS82]. Note that  $U_3(\mathbb{F}_p)$  is either the dihedral group  $D_4$  (when  $p = 2$ ) or the Heisenberg group  $H_{p^3}$  (when  $p > 2$ ).

The proof of Theorem A' is based on an alternative description of the  $p$ -Zassenhaus filtration in terms of Magnus algebra  $\mathbb{F}_p\langle\langle X_A \rangle\rangle$  of formal power series over  $\mathbb{F}_p$  in non-commuting variables  $X_a$ , where  $a$  ranges over a basis  $A$  of  $S$ . The Magnus homomorphism  $\Lambda: S \rightarrow \mathbb{F}_p\langle\langle X_A \rangle\rangle^\times$  is defined by  $a \mapsto 1 + X_a$  (see §5). Then  $S_n$  is the preimage under  $\Lambda$  of the multiplicative group of all formal power series  $1 + \sum_{|w| \geq n} c_w X_w$  (Proposition 6.2).

Behind the proof of Theorem A' is also a key observation from [EM11b], relating such intersection results with duality principles between profinite groups and subgroups of second cohomology groups (see Proposition 9.1 for the precise statement). In our case we consider the subgroup  $H^2(S/S_n)_{n-\text{Massey}}$  of  $H^2(S/S_n)$  and prove:

**Theorem B.** (a) *There is a natural perfect pairing*

$$S_n/S_{n+1} \times H^2(S/S_n)_{n-\text{Massey}} \rightarrow \mathbb{Z}/p.$$

(b) *There is a natural exact sequence*

$$0 \rightarrow H^2(S/S_n)_{n-\text{Massey}} \hookrightarrow H^2(S/S_n) \rightarrow H^2(S/S_{n+1}).$$

See Corollary 10.4 for a generalization of these facts to profinite groups  $G$  as above.

Finally, a method of Dwyer [Dwy75] expresses the central extensions corresponding to elements of  $H^2(S/S_n)_{n-\text{Massey}}$  by means of linear representations into  $U_n(\mathbb{Z}/p)$  (see §8), leading to Theorem A'.

Fundamental connections between the  $p$ -Zassenhaus filtration and Massey products were earlier observed and studied in the works of Morishita [Mor04], [Mor12] and Vogel [Vog05]; see also [Sta65, §5]. In fact, in the case  $p = 2$ ,  $n = 3$ , related connections were earlier studied in [GLMS03] under a different terminology (this was pointed out to me by Ján Mináč). Among the other recent important works on Massey products in Galois theory and arithmetic geometry are those by Sharifi [Sha07], Wickelgren, Hopkins ([Wic09], [Wic12], [HW12]), and Gärtner [Gär12].

I warmly thank Ján Mináč for many very inspiring discussions which motivated the present work and for his comments. I also thank A. Lubotzky, M. Schacher, N.D. Tan, and K. Wickelgren for their comments.

## 2. PRELIMINARIES ON BILINEAR PAIRINGS

First we recall some terminology and facts on bilinear maps. We fix a commutative ring  $R$ . A bilinear map  $(\cdot, \cdot): A \times B \rightarrow R$  of  $R$ -modules  $A$  and  $B$  is **non-degenerate** (resp., a **perfect pairing**) if the induced  $R$ -module homomorphisms  $A \rightarrow \text{Hom}_R(B, R)$  and  $B \rightarrow \text{Hom}_R(A, R)$  are

injective (resp., bijective). We say that a diagram of bilinear pairings and  $R$ -homomorphisms

$$(2.1) \quad \begin{array}{ccccc} A & \times & B & \xrightarrow{(\cdot, \cdot)} & R \\ \alpha \uparrow & & \downarrow \beta & & \parallel \\ A' & \times & B' & \xrightarrow{(\cdot, \cdot)'} & R \end{array}$$

**commutes** if  $(\alpha(a'), b) = (a', \beta(b))'$  for every  $a' \in A'$  and  $b \in B$ .

The proofs of the next two lemmas are straightforward:

**Lemma 2.1.** *Let  $(I, \leq)$  be a filtered set and for every  $i \in I$  let  $A_i \times B_i \rightarrow R$  be a perfect pairing. Let  $\alpha_{ij}: A_j \rightarrow A_i$ ,  $\beta_{ij}: B_i \rightarrow B_j$ , for  $i, j \in I$  with  $i \leq j$ , be homomorphisms which commute with the pairings, and are compatible in the natural sense. Then there is an induced perfect pairing  $\varprojlim A_i \times \varinjlim B_i \rightarrow R$ .*

**Lemma 2.2.** *Suppose that (2.1) commutes and the induced maps  $A \rightarrow \text{Hom}_R(B, R)$ ,  $B' \rightarrow \text{Hom}_R(A', R)$  are injective. Then (2.1) induces a non-degenerate bilinear map  $\text{Im}(\alpha) \times \text{Im}(\beta) \rightarrow R$ .*

**Lemma 2.3.** *Assume that every  $R$ -module is semi-simple. Suppose that the diagram (2.1) commutes,  $(\cdot, \cdot)$  is non-degenerate, and the induced map  $A' \mapsto \text{Hom}_R(B', R)$  is surjective. Then (2.1) induces a non-degenerate bilinear map  $\text{Coker}(\alpha) \times \text{Ker}(\beta) \rightarrow R$ .*

*Proof.* Set  $A'' = \text{Coker}(\alpha)$  and  $B'' = \text{Ker}(\beta)$ . The existence of an induced well-defined bilinear map  $A'' \times B'' \rightarrow R$  is straightforward. It is also immediate that the induced map  $B'' \rightarrow \text{Hom}_R(A'', R)$  is injective.

Finally, there is a commutative diagram with exact rows

$$\begin{array}{ccccccc} A' & \xrightarrow{\alpha} & A & \longrightarrow & A'' & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ \text{Hom}_R(B', R) & \longrightarrow & \text{Hom}_R(B, R) & \longrightarrow & \text{Hom}_R(B'', R) & & \end{array},$$

where the exactness at  $\text{Hom}_R(B, R)$  is by the semi-simplicity. By the snake lemma, the right vertical map is injective.  $\square$

### 3. MASSEY PRODUCTS

Recall that a **differential  $\mathbb{Z}$ -graded algebra** (DGA) over a ring  $R$  is a graded  $R$ -algebra  $C^\bullet = \bigoplus_{r \in \mathbb{Z}} C^r$  equipped with homomorphisms  $\partial^r: C^r \rightarrow C^{r+1}$  such that  $(C^\bullet, \bigoplus_{r \in \mathbb{Z}} \partial^r)$  is a complex satisfying the *Leibnitz rule*  $\partial^{r+s}(ab) = \partial^r(a)b + (-1)^r a \partial^s(b)$  for  $a \in C^r$ ,  $b \in C^s$ . Let  $H^i = \text{Ker}(\partial^i) / \text{Im}(\partial^{i-1})$

be the  $i$ -th cohomology group of  $C^\bullet$ . For an  $i$ -cocycle  $c$  let  $[c]$  be its cohomology class in  $H^i$ . Thus  $[c] = [c']$  will mean that  $c, c'$  are homogenous cocycles of equal degree and are cohomologous.

We fix an integer  $n \geq 2$ . We consider systems  $c_{ij} \in C^1$ , where  $1 \leq i \leq j \leq n$  and  $(i, j) \neq (1, n)$ . For any  $i, j$  satisfying  $1 \leq i \leq j \leq n$  (including  $(i, j) = (1, n)$ ) we may define

$$\tilde{c}_{ij} = - \sum_{r=i}^{j-1} c_{ir} c_{r+1,j} \in C^2.$$

One says that  $(c_{ij})$  is a **defining system of size  $n$**  in  $C^\bullet$  if  $\tilde{c}_{ij} = \partial c_{ij}$  for every  $1 \leq i \leq j \leq n$  with  $(i, j) \neq (1, n)$ . We also say that the defining system  $(c_{ij})$  is **on**  $c_{11}, \dots, c_{nn}$ . Note that then  $c_{ii}$  is a 1-cocycle,  $i = 1, 2, \dots, n$ . Further,  $\tilde{c}_{1n}$  is a 2-cocycle ([Kra66, p. 432], [Fen83, p. 233], [Efr12]).

**Lemma 3.1.** *Suppose that for every cocycles  $c_1, \dots, c_n \in C^1$  there is a defining system of size  $n$  on  $c_1, \dots, c_n$  in  $C^\bullet$ . Let  $1 \leq k < n$ . Then for every cocycles  $c_1, \dots, c_k \in C^1$  there is a defining system of size  $k$  on  $c_1, \dots, c_k$  such that in addition  $[\tilde{c}_{1k}] = 0$ .*

*Proof.* Choose arbitrary cocycles  $c_{k+1}, \dots, c_n \in C^1$  and a defining system  $(c_{ij})$  on  $c_1, \dots, c_k, c_{k+1}, \dots, c_n$ . Then  $(c_{ij})$ ,  $1 \leq i \leq j \leq k$ ,  $(i, j) \neq (1, k)$ , is a defining system on  $c_1, \dots, c_k$ . Moreover,  $\tilde{c}_{1k} = \partial c_{1k}$ , so  $[\tilde{c}_{1k}] = 0$ .  $\square$

The main objective of this section is Proposition 3.3 below. Its proof will be based on the following fact from [Fen83, Lemma 6.2.7], which is a variant of [Kra66, Lemma 20] (with different sign conventions). We note that while the latter results are stated in a topological setting, their proofs are at the level of general DGAs. A self-contained exposition of these results, also for cocycles of higher degrees, as well as of the multi-linearity of the Massey product (see below), is given in [Efr12].

**Proposition 3.2** (Fenn, Kraines). *Assume that for every  $1 \leq k < n$  and every defining system  $(d_{ij})$  of size  $k$  in  $C^\bullet$  one has  $[\tilde{d}_{1k}] = 0$ . Let  $(c_{ij}), (c'_{ij})$  be defining systems of size  $n$  in  $C^\bullet$  with  $[c_{ii}] = [c'_{ii}]$ ,  $i = 1, 2, \dots, n$ . Then  $[\tilde{c}_{1n}] = [\tilde{c}'_{1n}]$ .*

**Proposition 3.3.** *Suppose that for every cocycles  $c_1, \dots, c_n \in C^1$  there is a defining system on  $c_1, \dots, c_n$  in  $C^\bullet$ . Then for any two defining systems  $(c_{ij}), (c'_{ij})$  of size  $n$  with  $[c_{ii}] = [c'_{ii}]$ ,  $i = 1, 2, \dots, n$ , one has  $[\tilde{c}_{1n}] = [\tilde{c}'_{1n}]$ .*

*Proof.* We argue by induction on  $n$ . For  $n = 2$  this is immediate from the definition of  $\tilde{c}_{12}, \tilde{c}'_{12}$ .

For arbitrary  $n$ , the assumption holds also for smaller values of  $n$ , by Lemma 3.1. We obtain the last sentence of the proposition for smaller values of  $n$ . We need to verify the assumption of Proposition 3.2. So let  $1 \leq k < n$ , and consider a defining system  $(d_{ij})$  of size  $k$  in  $C^\bullet$ . Lemma 3.1 again yields a defining system  $(d'_{ij})$  of size  $k$  on  $d_{11}, \dots, d_{kk}$  such that in addition  $[\tilde{d}'_{1k}] = 0$ . Hence  $[\tilde{d}_{1k}] = [\tilde{d}'_{1k}] = 0$ , as required.  $\square$

Under the assumptions of Proposition 3.3, define the **Massey product**

$$(3.1) \quad \langle \cdot, \dots, \cdot \rangle: H^1 \times \dots \times H^1 \rightarrow H^2,$$

as follows: given cocycles  $c_1, \dots, c_n \in C^1$  we take a defining system  $(c_{ij})$  in  $C^\bullet$  with  $c_{11} = c_1, \dots, c_{nn} = c_n$ . As remarked above,  $\tilde{c}_{1n}$  is a 2-cocycle. We set  $\langle [c_1], \dots, [c_n] \rangle = [\tilde{c}_{1n}]$ . By Proposition 3.3, this map is well-defined. Moreover, it is multi-linear ([Fen83, Lemma 6.2.4], [Efr12]).

#### 4. FORMAL POWER SERIES

Let  $(A, \leq)$  be a set, considered as an alphabet, and  $A^*$  be the set of all finite words on  $A$ . We write  $\emptyset$  for the empty word, and  $|w|$  for the length of the word  $w$ .

We fix a commutative unital ring  $R$  and noncommuting variables  $X_a$ ,  $a \in A$ . The collection  $X_A$  of all formal expressions  $X_w = X_{a_1} \cdots X_{a_n}$ , with  $w = (a_1, \dots, a_n) \in A^*$ , forms a monoid under concatenation. Let  $R\langle\langle X_A \rangle\rangle$  be the ring of all formal power series  $\sum_{w \in A^*} c_w X_w$ , with  $c_w \in R$ . We denote by  $R\langle\langle X_A \rangle\rangle^\times$  its multiplicative group.

For a positive integer  $n$  let  $V_{n,R}$  be the subset of  $R\langle\langle X_A \rangle\rangle^\times$  consisting of all power series  $\sum_w c_w X_w$  such that  $c_\emptyset = 1$  and  $c_w = 0$  for every  $w$  with  $1 \leq |w| < n$ . Note that any  $1 + \alpha \in V_{n,R}$  has an inverse  $\sum_{k=0}^\infty (-1)^k \alpha^k$  in  $V_{n,R}$ , so  $V_{n,R}$  is a subgroup of  $R\langle\langle X_A \rangle\rangle^\times$ . We write  $V_{n,R}^m$  for the subgroup of  $V_{n,R}$  generated by all  $m$ -th powers, and  $[V_{n,R}, V_{k,R}]$  for the subgroup of  $V_{1,R}$  generated by all commutators  $[\gamma, \delta] = \gamma^{-1} \delta^{-1} \gamma \delta$ , with  $\gamma \in V_{n,R}$ ,  $\delta \in V_{k,R}$ .

**Lemma 4.1.** (a)  $[V_{n,R}, V_{k,R}] \leq V_{n+k,R}$ ;

(b) If  $mR = 0$ , then  $V_{n,R}^m \leq V_{n+1,R}$ .

*Proof.* For (a) let  $1 + \alpha \in V_{n,R}$  and  $1 + \beta \in V_{k,R}$ . Then

$$\begin{aligned} [1 + \alpha, 1 + \beta] &= (1 - \alpha + \alpha^2 - \dots)(1 - \beta + \beta^2 - \dots)(1 + \alpha)(1 + \beta) \\ &\in 1 + R\langle\langle X_A \rangle\rangle \alpha \beta R\langle\langle X_A \rangle\rangle + R\langle\langle X_A \rangle\rangle \beta \alpha R\langle\langle X_A \rangle\rangle \leq V_{n+k,R}. \end{aligned}$$

For (b), use the (non-commutative) binomial formula.  $\square$

## 5. FREE PROFINITE GROUPS

We recall from [FJ08, §17.4] the following terminology and facts on free profinite groups.

Let  $G$  be a profinite group and  $A$  a set. A map  $\varphi: A \rightarrow G$  **converges to 1** if for every open normal subgroup  $M$  of  $G$ , the set  $A \setminus \varphi^{-1}(M)$  is finite.

Let  $S$  be a profinite group. We say that  $S$  is a **free profinite group on basis**  $A$  with respect to a map  $\iota: A \rightarrow S$  if

- (i)  $\iota: A \rightarrow S$  converges to 1 and  $\iota(A)$  generates  $S$ ;
- (ii) For every profinite group  $G$  and a continuous map  $\varphi: A \rightarrow G$  converging to 1, there is a unique continuous homomorphism  $\hat{\varphi}: S \rightarrow G$  with  $\varphi = \hat{\varphi} \circ \iota$  on  $A$ .

A free profinite group on  $A$  exists, and is unique up to a continuous isomorphism. We denote it by  $S_A$ . Necessarily,  $\iota$  is injective, and we identify  $A$  with its image in  $S_A$ . The group  $S_A$  is projective, whence has cohomological dimension  $\leq 1$  [NSW08, Cor. 3.5.16].

Now let  $R$  be a profinite unital ring. The map  $\sum_w c_w X_w \mapsto (c_w)_w$  identifies  $R\langle\langle X_A \rangle\rangle$  with  $R^{A^*}$ . This induces on the additive group of  $R\langle\langle X_A \rangle\rangle$  a profinite topology. Moreover, the multiplication map in  $R\langle\langle X_A \rangle\rangle$  is continuous, making it a profinite topological ring.

Now take  $A$  finite. The ring  $R\langle\langle X_A \rangle\rangle$  is profinite ring, so  $R\langle\langle X_A \rangle\rangle^\times$  is a profinite group. Hence the map  $a \mapsto 1 + X_a$ ,  $a \in A$ , extends to the (continuous) **Magnus homomorphism**  $\Lambda_{S_A, R}: S_A \rightarrow R\langle\langle X_A \rangle\rangle^\times$ .

This generalizes to arbitrary  $A$  as follows: Let  $B$  be a finite subset of  $A$ . The map  $\varphi: A \rightarrow S_B$ , given by  $a \mapsto a$  for  $a \in B$ , and  $a \mapsto 1$  for  $a \in A \setminus B$ , converges to 1. It extends to a unique continuous epimorphism  $S_A \rightarrow S_B$ . Also, there is a continuous  $R$ -algebra epimorphism  $R\langle\langle X_A \rangle\rangle \rightarrow R\langle\langle X_B \rangle\rangle$ , given by  $X_b \mapsto X_b$  for  $b \in B$  and  $X_a \mapsto 0$  for  $a \in A \setminus B$ . Then

$$S_A = \varprojlim S_B, \quad R\langle\langle X_A \rangle\rangle = \varprojlim R\langle\langle X_B \rangle\rangle, \quad R\langle\langle X_A \rangle\rangle^\times = \varprojlim R\langle\langle X_B \rangle\rangle^\times,$$

where  $B$  ranges over all finite subsets of  $A$ . We now define  $\Lambda_{S_A, R}: S_A \rightarrow R\langle\langle X_A \rangle\rangle^\times$  to be the inverse limit of the maps  $\Lambda_{S_B, R}$ . Thus  $\Lambda_{S_A, R}(a) = 1 + X_a$  for  $a \in A$ .

From now on we abbreviate  $S = S_A$ . For  $\sigma \in S$  we set

$$\Lambda_{S, R}(\sigma) = \sum_{w \in A^*} \epsilon_{w, R}(\sigma) X_w$$

with  $\epsilon_{w, R}(\sigma) \in R$ . Thus  $\epsilon_{\emptyset, R}(\sigma) = 1$ .

For a positive integer  $n$  let  $S_{n,R} = \Lambda_{S,R}^{-1}(V_{n,R})$ . It is closed subgroup of  $S$ , and  $S_{1,R} = S$ . Also,  $S_{n,R} = \varprojlim (S_B)_{n,R}$ , with  $B$  ranging over all finite subsets of  $A$ . The next lemma records a few well-known facts.

**Lemma 5.1.** *Let  $w \in A^*$ .*

- (a) *For  $\sigma, \tau \in S$  one has  $\epsilon_{w,R}(\sigma\tau) = \sum \epsilon_{w_1,R}(\sigma)\epsilon_{w_2,R}(\tau)$ , where the sum is over all  $w_1, w_2 \in A^*$  with  $w = w_1w_2$ .*
- (b) *For  $n = |w|$ , the restriction  $\epsilon_{w,R}: S_{n,R} \rightarrow R$  is a homomorphism.*
- (c) *For  $a \in A$ , the map  $\epsilon_{(a),R}: S \rightarrow R$  is a homomorphism.*
- (d)  *$\epsilon_{(a),R}(a) = 1$  for  $a \in A$  and  $\epsilon_{(a),R}(a') = 0$  for  $a, a' \in A$  distinct.*

*Proof.* (a) is a restatement of  $\Lambda_{S,R}(\sigma\tau) = \Lambda_{S,R}(\sigma)\Lambda_{S,R}(\tau)$ . (b) follows from (a), and (c) is a special case of (b). (d) is immediate from the definition.  $\square$

## 6. THE FILTRATION $S_{n,\mathbb{Z}/m}$

Let  $S = S_A$  be as before, and assume that  $R = \mathbb{Z}/m$  for an integer  $m \geq 2$ . Lemma 4.1 implies that

$$(6.1) \quad S_{n,\mathbb{Z}/m}^m[S, S_{n,\mathbb{Z}/m}] \leq S_{n+1,\mathbb{Z}/m}.$$

For  $n = 1$ , this is an equality:

**Lemma 6.1.**  $S^m[S, S] = S_{2,\mathbb{Z}/m}$ .

*Proof.* By (6.1),  $S^m[S, S] \leq S_{2,\mathbb{Z}/m}$ .

For the converse, we may use an inverse limit argument to assume that  $A$  is finite. Let  $\bar{S} = S/S^m[S, S]$  and let  $\bar{\Lambda}_{S,\mathbb{Z}/m}: \bar{S} \rightarrow V_{1,\mathbb{Z}/m}/V_{2,\mathbb{Z}/m}$  be the homomorphism induced by  $\Lambda_{S,\mathbb{Z}/m}$ . Use Lemma 4.1 to obtain that  $V_{1,\mathbb{Z}/m}/V_{2,\mathbb{Z}/m}$  is a free  $\mathbb{Z}/m$ -module on generators  $(1 + X_a)V_{2,\mathbb{Z}/m}$ ,  $a \in A$ . Since  $\bar{S}$  is abelian of exponent  $m$ , we may define a homomorphism  $\lambda: V_{1,\mathbb{Z}/m}/V_{2,\mathbb{Z}/m} \rightarrow \bar{S}$  by mapping this generator to the image  $\bar{a}$  of  $a$  in  $\bar{S}$ . Then  $(\lambda \circ \bar{\Lambda}_{S,\mathbb{Z}/m})(\bar{a}) = \bar{a}$  for  $a \in A$ , implying that  $\lambda \circ \bar{\Lambda}_{S,\mathbb{Z}/m} = \text{id}_{\bar{S}}$  and  $\bar{\Lambda}_{S,\mathbb{Z}/m}$  is injective. But  $S_{2,\mathbb{Z}/m}/S^m[S, S]$  is mapped trivially by  $\bar{\Lambda}_{S,\mathbb{Z}/m}$ , and therefore is trivial.  $\square$

Now let  $m = p$  prime. For a profinite group  $G$  let  $I_{\mathbb{F}_p}(G)$  be the augmentation ideal in the complete group ring  $\mathbb{F}_p[[G]]$ , i.e., the closed ideal generated by all elements  $g - 1$ , with  $g \in G$ . When  $G$  is finite (whence discrete), a theorem of Jennings and Brauer ([Jen41, Th. 5.5], [DDMS, Th. 12.9]) identifies  $G \cap (1 + I_{\mathbb{F}_p}(G)^n)$  with the  $n$ th term  $G_n$  in the Zassenhaus filtration of  $G$ ,  $n \geq 1$ . An inverse limit argument extends this to arbitrary profinite groups  $G$ .



The map  $1 + \sum_{|w| \geq n} c_w X_w \mapsto (c_w)_{|w|=n}$  induces a group isomorphism  $V_{n, \mathbb{F}_p} / V_{n+1, \mathbb{F}_p} \xrightarrow{\sim} \prod_{w \in A^*, |w|=n} \mathbb{F}_p$ . When  $A$  is finite,  $V_{1, \mathbb{F}_p} / V_{n, \mathbb{F}_p}$  is therefore a finite  $p$ -group for every  $n$ , so  $V_{1, \mathbb{F}_p} = \varprojlim V_{1, \mathbb{F}_p} / V_{n, \mathbb{F}_p}$  is a pro- $p$  group.

**Proposition 6.2.**  $S_n = S_{n, \mathbb{F}_p}$ .

*Proof.* By an inverse limit argument, we may assume that the basis  $A$  is finite. Let  $\bar{S}$  be the maximal pro- $p$  quotient of  $S$ . It is a free pro- $p$  group. By the definition of the Zassenhaus filtration,  $S/S_n$  has a  $p$ -power exponent. Hence the preimage of  $\bar{S}_n$  under the epimorphism  $S \rightarrow \bar{S}$  is  $S_n$ .

Also,  $\Lambda_{S, \mathbb{F}_p}$  breaks via a homomorphism  $\bar{\Lambda}_{S, \mathbb{F}_p}: \bar{S} \rightarrow V_{1, \mathbb{F}_p}$ . It extends to a continuous  $\mathbb{F}_p$ -algebra homomorphism  $\bar{\Lambda}_{\bar{S}, \mathbb{F}_p}: \mathbb{F}_p[[\bar{S}]] \rightarrow \mathbb{F}_p\langle\langle X_A \rangle\rangle$ , which by [Koc02, Th. 7.16], is an isomorphism. Let  $J = V_{1, \mathbb{F}_p} - 1$  be the ideal of all power series in  $\mathbb{F}_p\langle\langle X_A \rangle\rangle$  with constant term 0. Using the identity  $\sigma\tau - 1 = (\sigma - 1)(\tau - 1) + (\sigma - 1) + (\tau - 1)$  for  $\sigma, \tau \in \bar{S}$  we see that  $\bar{\Lambda}_{\bar{S}, \mathbb{F}_p}$  maps  $I_{\mathbb{F}_p}(\bar{S})$  onto  $J$ . Therefore it maps  $1 + I_{\mathbb{F}_p}(\bar{S})^n$  bijectively onto  $1 + J^n = V_{n, \mathbb{F}_p}$ . By the Jennings–Brauer theorem,  $\bar{S}_n$  is therefore the preimage of  $V_{n, \mathbb{F}_p}$  in  $\bar{S}$  under  $\bar{\Lambda}_{\bar{S}, \mathbb{F}_p}$ . We conclude that  $S_n$  is the preimage of  $V_{n, \mathbb{F}_p}$  in  $S$  under  $\Lambda_{S, \mathbb{F}_p}$ , i.e.,  $S_n = S_{n, \mathbb{F}_p}$ .  $\square$

**Lemma 6.3.** Let  $c_1, \dots, c_n: S = S_A \rightarrow \mathbb{F}_p$  be continuous homomorphisms and  $B = \{b_1, \dots, b_n\}$  a set of size  $n$ . There is a continuous homomorphism  $\phi: S_A \rightarrow S_B$  such that  $\epsilon_{(b_i), \mathbb{F}_p}^B \circ \phi = c_i$ ,  $i = 1, 2, \dots, n$ , where  $\epsilon^B$  denotes the Magnus coefficient with respect to  $S_B$ .

*Proof.* An inverse limit argument reduces this to the case where  $A$  is finite. For every  $a \in A$  and  $1 \leq i \leq n$  choose  $\hat{c}_i(a) \in \mathbb{Z}$  with  $c_i(a) = \hat{c}_i(a) \pmod{p\mathbb{Z}}$ . The map  $A \rightarrow S_B$ ,  $a \mapsto \prod_{i=1}^n b_i^{\hat{c}_i(a)}$ , extends to a continuous homomorphism  $\phi: S_A \rightarrow S_B$ . Then  $\epsilon_{(b_i), \mathbb{F}_p}^B(\phi(a)) = c_i(a)$  for every  $a \in A$  and  $1 \leq i \leq n$ , and the assertion follows.  $\square$

## 7. UNIPOTENT MATRICES

Consider integers  $n \geq 2$  and  $d \geq 0$ , and let  $R$  be a (discrete) finite ring. Let  $T_{n,d}(R)$  be the set of all  $n \times n$  matrices  $(a_{ij})$  over  $R$  with the  $(1, n)$  entry omitted and such that  $a_{ij} = 0$  for  $j - i \leq d - 1$  (in particular,  $(a_{ij})$  is upper-triangular). It is an  $R$ -algebra with respect to the standard operations. Note that  $T_{n,d}T_{n,d'} \subseteq T_{n,d+d'}$ . Furthermore, for every entry  $(i, j) \neq (1, n)$  we have  $j - i \leq n - 2$ . Hence  $T_{n,d} = \{0\}$  for  $n - 1 \leq d$ . We denote the  $n \times n$  identity matrix with the  $(1, n)$  entry omitted by  $I_n$ .

Let  $U_n(R)$  be the group of all upper-triangular unipotent  $n \times n$  matrices over  $R$ . Let  $\bar{U}_n(R) = I_n + T_{n,1}(R)$  be the group of all unipotent (punctured)

matrices in  $T_{n,0}$ . Let  $\pi: U_n(R) \rightarrow \bar{U}_n(R)$  be the obvious forgetful epimorphism. Its kernel consists of all matrices in  $U_n(R)$  which are zero except for the main diagonal and at the entry  $(1, n)$ , and is therefore isomorphic to the additive group of  $R$ . We obtain a central extension of groups

$$0 \rightarrow R \rightarrow U_n(R) \xrightarrow{\pi} \bar{U}_n(R) \rightarrow 1.$$

We endow  $U_n(R)$ ,  $\bar{U}_n(R)$  with the discrete topologies.

For the rest of this section we set  $S = S_A$  and  $R = \mathbb{Z}/m$ , with  $m \geq 2$ .

**Proposition 7.1.** *Every continuous homomorphism  $\gamma: S \rightarrow \bar{U}_n(R)$  is trivial on  $S_{n-1,R}$ .*

*Proof.* An inverse limit argument reduces this to the case where  $A$  is finite.

For  $w = (a_1, \dots, a_d) \in A^*$  we set  $M_w = \prod_{j=1}^d (\gamma(a_j) - I_n) \in T_{n,d}$  (where  $M_\emptyset = I_n$ ). Since  $T_{n,d} = \{0\}$  for  $n-1 \leq d$ , we may therefore define a unital  $R$ -algebra homomorphism  $h: R\langle\langle X_A \rangle\rangle \rightarrow T_{n,0}(R)$  by

$$h\left(\sum_{w \in A^*} c_w X_w\right) = \sum_{\substack{w \in A^* \\ |w| \leq n-2}} c_w M_w.$$

Note that  $h$  is continuous with respect to the profinite topology on  $R\langle\langle X_A \rangle\rangle$  and the discrete topology on  $T_{n,0}(R)$ . The restriction of  $h$  to  $V_{1,R}$  is a continuous group homomorphism  $h: V_{1,R} \rightarrow \bar{U}_n(R) \subseteq T_{n,0}(R)$ . One has  $\gamma = h \circ \Lambda_{S,R}$  on  $A$ , whence on  $S$ . For  $\sigma \in S_{n-1,R}$  this gives  $\gamma(\sigma) = (h \circ \Lambda_{S,R})(\sigma) = I_n$ .  $\square$

**Corollary 7.2.** *Every continuous homomorphism  $\gamma: S \rightarrow U_n(R)$  is trivial on  $S_{n,R}$ .*

*Proof.* Embed  $U_n(R)$  in  $\bar{U}_{n+1}(R)$  and use Proposition 7.1.  $\square$

Given a continuous homomorphism  $\bar{\gamma}: S/S_{n-1,R} \rightarrow \bar{U}_n(R)$  we write  $U_n(R) \times_{\bar{U}_n(R)} (S/S_{n-1,R})$  for the fiber product with respect to  $\pi$  and  $\bar{\gamma}$ .

**Lemma 7.3.** *Let  $N$  and  $M_0$  be closed normal subgroup of  $S$  such that  $N \leq S_{n-1,R} \cap M_0$ . The following conditions are equivalent:*

- (1) *there exist a continuous homomorphism  $\bar{\gamma}: S/S_{n-1,R} \rightarrow \bar{U}_n(R)$  and a continuous homomorphism*

$$\hat{\Phi}: S/N \rightarrow U_n(R) \times_{\bar{U}_n(R)} (S/S_{n-1,R})$$

*which commutes with the projections to  $S/S_{n-1,R}$ , and such that  $M_0/N = \text{Ker}(\hat{\Phi})$ .*

- (2) *there exists a continuous homomorphism  $\Phi: S/N \rightarrow U_n(R)$  such that  $M_0/N = \text{Ker}(\Phi) \cap (S_{n-1,R}/N)$ ;*

- (3) *there is a closed normal subgroup  $M$  of  $S$  containing  $N$  such that  $S/M$  embeds in  $U_n(R)$  and  $M_0 = M \cap S_{n-1,R}$ .*

*Proof.* (1) $\Rightarrow$ (2): For  $i = 1, 2$  let  $\text{pr}_i$  be the projection on the  $i$ -th coordinate of the fiber product, and  $\text{pr}: S \rightarrow S/N$  the natural map. For  $\hat{\Phi}$  as in (1), we set  $\Phi = \text{pr}_1 \circ \hat{\Phi}$ . We get a commutative diagram

$$\begin{array}{ccccc}
 S & \xrightarrow{\text{pr}} & S/N & & \\
 & & \searrow \hat{\Phi} & \nearrow & \\
 & & U_n(R) \times_{\bar{U}_n(R)} (S/S_{n-1,R}) & \xrightarrow{\text{pr}_2} & S/S_{n-1,R} \\
 & \searrow \Phi & \downarrow \text{pr}_1 & & \downarrow \bar{\gamma} \\
 & & U_n(R) & \xrightarrow{\pi} & \bar{U}_n(R)
 \end{array}$$

Further,  $M_0/N = \text{Ker}(\hat{\Phi}) = \text{Ker}(\Phi) \cap (S_{n-1,R}/N)$ .

(2) $\Rightarrow$ (1): Given  $\Phi$  as in (2), the homomorphism  $\pi \circ \Phi \circ \text{pr}: S \rightarrow \bar{U}_n(R)$  factors via a continuous homomorphism  $\bar{\gamma}: S/S_{n-1,R} \rightarrow \bar{U}_n(R)$ , by Proposition 7.1. Thus the outer part of the diagram above commutes. The universal property of the fiber product yields a continuous homomorphism  $\hat{\Phi}$  making the two triangles commutative. We have

$$M_0/N = \text{Ker}(\Phi) \cap (S_{n-1,R}/N) = \text{Ker}(\hat{\Phi}).$$

(2) $\Leftrightarrow$ (3): Take  $\text{Ker}(\Phi) = M/N$ . □

One has the following important connection between homomorphisms as discussed above and words:

**Lemma 7.4.** *Let  $w = (a_1, \dots, a_n) \in A^*$ . Define maps  $\gamma_1, \gamma_2: S \rightarrow U_{n+1}(R)$  by*

$$\gamma_1(\sigma)_{ij} = \epsilon_{(a_i, \dots, a_{j-1}), R}(\sigma), \quad \gamma_2(\sigma)_{ij} = (-1)^{j-i} \epsilon_{(a_i, \dots, a_{j-1}), R}(\sigma)$$

*for  $\sigma \in S$  and  $i < j$  (the other entries being obvious). Then  $\gamma_1, \gamma_2$  are continuous group homomorphisms.*

*Proof.* For  $\gamma_1$  use Lemma 5.1(a). For  $\gamma_2$  observe that the map  $(a_{ij}) \mapsto ((-1)^{j-i} a_{ij})$  is an automorphism of  $U_{n+1}(R)$ , and compose it with  $\gamma_1$ . □

## 8. MASSEY PRODUCTS FOR INHOMOGENOUS COCHAINS

Let  $G$  be a profinite group which acts trivially and continuously on the unital finite (discrete) ring  $R$ . The complex  $(C^\bullet(G, R), \partial)$  of continuous inhomogenous  $G$ -cochains into the additive group of  $R$ , and  $C^r(G, R) = 0$

for  $r < 0$ , is a DGA with the cup product [NSW08, Ch. I, §2]. We recall that for  $c \in C^1(G, R)$  and  $\sigma, \tau \in G$  one has  $(\partial c)(\sigma, \tau) = c(\sigma) + c(\tau) - c(\sigma\tau)$ . Thus the 1-cocycles are the continuous homomorphisms  $c: G \rightarrow R$ . We now focus on defining systems in  $C^\bullet(G, R)$ .

As observed by Dwyer [Dwy75, §2] in the discrete context, one may view defining systems of size  $n$  in  $C^\bullet(G, R)$  as continuous homomorphisms  $G \rightarrow \bar{U}_{n+1}(R)$ , as follows. Define a bijection between the systems of 1-cochains  $c_{ij} \in C^1(G, R)$ ,  $1 \leq i \leq j \leq n$ ,  $(i, j) \neq (1, n)$ , and the continuous maps  $\bar{\gamma}: G \rightarrow \bar{U}_{n+1}(R)$  by

$$\bar{\gamma}(\sigma)_{ij} = (-1)^{j-i} c_{i,j-1}(\sigma)$$

for  $\sigma \in G$  and  $1 \leq i < j \leq n+1$ ,  $(i, j) \neq (1, n+1)$  (where the other entries are obvious). Under this bijection one has for  $\sigma, \tau \in G$ ,

$$(8.1) \quad \tilde{c}_{il}(\sigma, \tau) = - \sum_{r=i}^{l-1} c_{ir}(\sigma) c_{r+1,l}(\tau) = (-1)^{l-i} \sum_{k=i+1}^l \bar{\gamma}(\sigma)_{ik} \bar{\gamma}(\tau)_{k,l+1}.$$

**Lemma 8.1.**  *$\bar{\gamma}$  is a homomorphism if and only if  $(c_{ij})$  is a defining system of size  $n$  for  $C^\bullet(G, R)$ .*

*Proof.* The map  $\bar{\gamma}$  is a homomorphism if and only if for every  $\sigma, \tau \in G$  and  $1 \leq i \leq l \leq n$  with  $(i, l) \neq (1, n)$ ,

$$\bar{\gamma}(\sigma\tau)_{i,l+1} = \bar{\gamma}(\tau)_{i,l+1} + \sum_{k=i+1}^l \bar{\gamma}(\sigma)_{ik} \bar{\gamma}(\tau)_{k,l+1} + \bar{\gamma}(\sigma)_{i,l+1}.$$

By (8.1), this means that  $c_{il}(\sigma\tau) = c_{il}(\tau) - \tilde{c}_{il}(\sigma, \tau) + c_{il}(\sigma)$ . Equivalently,  $\tilde{c}_{il}(\sigma, \tau) = (\partial c_{il})(\sigma, \tau)$ , i.e.,  $(c_{ij})$  is a defining system.  $\square$

**Remark 8.2.** The same formula gives a bijection between the systems  $c_{ij} \in C^1(G, R)$ ,  $1 \leq i \leq j \leq n$ , and the continuous maps  $\gamma: G \rightarrow U_{n+1}(R)$ . Moreover,  $\gamma$  is a homomorphism if and only if  $(c_{ij})$  is a defining system such that in addition  $\tilde{c}_{1n} = \partial c_{1n}$ .

The following fact (with different sign conventions) is stated without a proof in [Dwy75, p. 182, Remark]; see also [Wic12, §2.4].

**Proposition 8.3.** *Let  $\bar{\gamma}: G \rightarrow \bar{U}_{n+1}(R)$  correspond to a defining system  $(c_{ij})$  as above. The central extension associated with  $(-1)^{n-1} \tilde{c}_{1n}$  is*

$$0 \rightarrow R \rightarrow U_{n+1}(R) \times_{\bar{U}_{n+1}(R)} G \rightarrow G \rightarrow 1,$$

where the fiber product is with respect to  $\pi$  and  $\bar{\gamma}$ .

*Proof.* Since  $(-1)^{n-1}\tilde{c}_{1n}$  is a 2-cocycle,  $B = R \times G$  is a group with respect to the product  $(r, \sigma) * (s, \tau) = (r + s + (-1)^{n-1}\tilde{c}_{1n}(\sigma, \tau), \sigma\tau)$ . Then the central extension corresponding to  $(-1)^{n-1}\tilde{c}_{1n}$  is [NSW08, Th. 1.2.4]

$$0 \rightarrow R \rightarrow B \rightarrow G \rightarrow 1.$$

The map  $h: U_{n+1}(R) \times_{\bar{U}_{n+1}(R)} G \rightarrow B$ ,  $((a_{ij}), \sigma) \mapsto (a_{1,n+1}, \sigma)$ , is a bijection commuting with the projections to  $G$ . To show that  $h$  is a homomorphism, take  $((a_{ij}), \sigma), ((b_{ij}), \tau) \in U_{n+1}(R) \times_{\bar{U}_{n+1}(R)} G$ . Thus

$$a_{ij} = \bar{\gamma}(\sigma)_{ij} = (-1)^{j-i}c_{i,j-1}(\sigma), \quad b_{ij} = \bar{\gamma}(\tau)_{ij} = (-1)^{j-i}c_{i,j-1}(\tau)$$

for  $1 \leq i < j \leq n+1$ ,  $(i, j) \neq (1, n+1)$ . By (8.1),  $\sum_{k=2}^n a_{1k}b_{k,n+1} = (-1)^{n-1}\tilde{c}_{1n}(\sigma, \tau)$ . Hence

$$\begin{aligned} h\left(((a_{ij}), \sigma)((b_{ij}), \tau)\right) &= \left(\sum_{k=1}^{n+1} a_{1k}b_{k,n+1}, \sigma\tau\right) \\ &= \left(a_{1,n+1} + b_{1,n+1} + (-1)^{n-1}\tilde{c}_{1n}(\sigma, \tau), \sigma\tau\right) = h\left(((a_{ij}), \sigma)\right) * h\left(((b_{ij}), \tau)\right). \end{aligned}$$

□

For the rest of the paper we set again  $R = \mathbb{Z}/m$ . Let  $S = S_A$  and let  $N$  be a normal closed subgroup of  $S$  contained in  $S_{n,\mathbb{Z}/m}$ , with  $n \geq 2$ .

**Proposition 8.4.** *Given continuous homomorphisms  $c_1, \dots, c_n: S \rightarrow \mathbb{Z}/m$ , there is a defining system  $(\bar{c}_{ij})$  of size  $n$  in  $C^\bullet(S/N, \mathbb{Z}/m)$  with  $c_i = \inf_S(\bar{c}_i)$ ,  $i = 1, 2, \dots, n$ .*

*Proof.* Let  $S_B$  be a free profinite group on a set  $B = \{b_1, b_2, \dots, b_n\}$  of  $n$  elements. We write  $\epsilon_{w,\mathbb{Z}/m}^B$  for the corresponding Magnus coefficients. Lemma 6.3 yields a continuous homomorphism  $\phi: S \rightarrow S_B$  such that  $\epsilon_{(b_i),\mathbb{Z}/m}^B \circ \phi = c_i$ ,  $i = 1, 2, \dots, n$ . We define a map  $\gamma': S_B \rightarrow U_{n+1}(\mathbb{Z}/m)$  by  $\gamma'(\sigma')_{ij} = (-1)^{j-i}\epsilon'_{(b_i, \dots, b_{j-1}),\mathbb{Z}/m}(\sigma')$  for  $i < j$  and  $\sigma' \in S_B$ . By Lemma 7.4,  $\gamma'$  is a continuous homomorphism. The composition  $\gamma = \pi \circ \gamma' \circ \phi: S \rightarrow \bar{U}_{n+1}(\mathbb{Z}/m)$  is also a continuous homomorphism. By Proposition 7.1, it factors via a continuous homomorphism  $\bar{\gamma}: S/N \rightarrow \bar{U}_{n+1}(\mathbb{Z}/m)$ :

$$\begin{array}{ccccc} S & \xrightarrow{\phi} & S_B & \xrightarrow{\gamma'} & U_{n+1}(\mathbb{Z}/m) \\ \downarrow & & \searrow \gamma & & \downarrow \pi \\ S/N & \xrightarrow{\bar{\gamma}} & & & \bar{U}_{n+1}(\mathbb{Z}/m). \end{array}$$

Let  $(\bar{c}_{ij})$  be the defining system of size  $n$  on  $C^\bullet(S/N, \mathbb{Z}/m)$  associated with  $\bar{\gamma}$ , in the sense of Lemma 8.1. Then for  $\sigma \in S$  and  $1 \leq i \leq n$ ,

$$(\inf_S(\bar{c}_{ii}))(\sigma) = -\gamma_{i,i+1}(\sigma) = -\gamma'_{i,i+1}(\phi(\sigma)) = \epsilon_{(b_i), \mathbb{Z}/m}^B(\phi(\sigma)) = c_i(\sigma). \quad \square$$

For a profinite group  $G$  acting trivially on  $\mathbb{Z}/m$ , let  $H^i(G) = H^i(G, \mathbb{Z}/m)$  be the  $i$ -th cohomology group corresponding to the DGA  $C^\bullet(G, \mathbb{Z}/m)$  over  $\mathbb{Z}/m$ . In view of Proposition 8.4, the assumption of Proposition 3.3 is satisfied for  $C^\bullet(S/N, \mathbb{Z}/m)$ . Consequently, as explained in §3, there is a well-defined Massey product

$$\langle \cdot, \dots, \cdot \rangle: H^1(S/N)^n \rightarrow H^2(S/N).$$

This was earlier shown using a different method by Vogel [Vog05, Th. A3] for  $m = p$  prime. We write  $H^2(S/N)_{n\text{-Massey}}$  for the image of this map.

**Example 8.5.** For  $n = 2$  and  $\chi_1, \chi_2 \in H^1(S/N)$  we have by construction  $\langle \chi_1, \chi_2 \rangle = -\chi_1 \cup \chi_2 \in H^2(S/N)$ , where  $\cup$  denotes the cup product. Thus in the terminology of [CEM12],  $H^2(S/N)_{2\text{-Massey}} = H^2(S/N)_{\text{dec}}$ .

For  $a \in A$  we may consider  $\epsilon_{(a), \mathbb{Z}/m} \in H^1(S)$  also as an element of  $H^1(S/N)$  (see Lemma 6.1). With this convention we have

**Lemma 8.6.** *The Massey products  $\psi_w = \langle \epsilon_{(a_1), \mathbb{Z}/m}, \dots, \epsilon_{(a_n), \mathbb{Z}/m} \rangle$ , where  $w = (a_1, \dots, a_n) \in A^*$ , generate  $H^2(S/N)_{n\text{-Massey}}$ .*

*Proof.* In view of Lemma 5.1(d),  $\epsilon_{(a), \mathbb{Z}/m}$ , where  $a \in A$ , generate  $H^1(S/N) = \text{Hom}(S/N, \mathbb{Z}/m)$ . Now use the multi-linearity of the Massey product.  $\square$

## 9. COHOMOLOGICAL DUALITY

Let  $G$  be a profinite group acting trivially on  $\mathbb{Z}/m$  and let  $N$  be a closed normal subgroup of  $G$ . One has the 5-term exact sequence for the lower cohomology groups with coefficients in  $\mathbb{Z}/m$  [NSW08, Prop. 1.6.7]:

$$0 \rightarrow H^1(G/N) \xrightarrow{\inf} H^1(G) \xrightarrow{\text{res}} H^1(N)^G \xrightarrow{\text{trg}} H^2(G/N) \xrightarrow{\inf} H^2(G).$$

When  $N \leq G^m[G, G]$ , the inflation map  $\inf: H^1(G/N) \rightarrow H^1(G)$  is surjective, so the transgression map  $\text{trg}$  identifies  $H^1(N)^G$  with  $\text{Ker}(H^2(G/N) \xrightarrow{\inf} H^2(G))$ . Therefore [EM11a, Cor. 2.2] gives a non-degenerate bilinear map

$$(\cdot, \cdot)': N/N^m[G, N] \times \text{Ker}(H^2(G/N) \xrightarrow{\inf} H^2(G)) \rightarrow \mathbb{Z}/m, \\ (\sigma N^m[G, N], \alpha)' = (\text{trg}^{-1}(\alpha))(\sigma).$$

We will need the following result from [EM11b, Prop. 3.2]. Note that while it is stated for  $m$  a prime power, this is not needed in its proof.

**Proposition 9.1.** *Let  $T, T_0$  be closed normal subgroups of  $G$  such that  $T^m[G, T] \leq T_0 \leq T \leq G^m[G, G]$ . Let  $H$  be a subgroup of  $H^2(G/T)$  and  $H_0$  a set of generators of  $H \cap \text{trg}(H^1(T)^G) = \text{Ker}(\text{inf}: H \rightarrow H^2(G))$ . The following conditions are equivalent:*

(a)  $(\cdot, \cdot)'$  (for  $N = T$ ) induces a non-degenerate bilinear map

$$T/T_0 \times \text{Ker}(H \xrightarrow{\text{inf}} H^2(G)) \rightarrow \mathbb{Z}/m;$$

(b) there is an exact sequence

$$0 \rightarrow \text{Ker}(H^2(G/T) \xrightarrow{\text{inf}} H^2(G/T_0)) \rightarrow H \xrightarrow{\text{inf}} H^2(G);$$

(c)  $T_0 = \bigcap \text{Ker}(\Psi)$ , with  $\Psi$  ranging over all homomorphisms with a commutative diagram

$$\begin{array}{ccccccc} & & & & G & & \\ & & & & \downarrow & & \\ \omega : & 0 & \longrightarrow & \mathbb{Z}/m & \longrightarrow & C & \longrightarrow G/T \longrightarrow 1, \\ & & & & \swarrow \Psi & & \end{array}$$

where  $\omega$  is a central extension associated with some element of  $H_0$ .

We now restrict ourselves to the case where  $G$  is a free profinite group  $S = S_A$ . Let  $N$  be a normal subgroup of  $S$  contained in  $S_{n, \mathbb{Z}/m}$ , where  $n \geq 2$ . Then  $N \leq S_{2, \mathbb{Z}/m} = S^m[S, S]$ , by Lemma 6.1. As  $H^2(S) = 0$ , we obtain a non-degenerate bilinear map

$$(9.1) \quad (\cdot, \cdot)': N/N^m[S, N] \times H^2(S/N) \rightarrow \mathbb{Z}/m.$$

Variants of the following fundamental fact were proved by Dwyer [Dwy75, Prop. 4.1], Fenn and Sjerve [FS84, Th. 6.6], Morishita [Mor04, Cor. 2.2.3], Vogel [Vog05, Th. A3] and Wickelgren [Wic09, Prop. 2.3.7]. We prove it here in our terminology and setup. Let  $\psi_w$  be as in Lemma 8.6.

**Theorem 9.2.** *For  $\sigma \in N$  and  $w \in A^*$  one has  $(\bar{\sigma}, \psi_w)' = \epsilon_{w, \mathbb{Z}/m}(\sigma)$ .*

*Proof.* Let  $w = (a_1, \dots, a_n)$ . Lemma 7.4 gives a continuous homomorphism  $\gamma: S \rightarrow \text{U}_{n+1}(\mathbb{Z}/m)$ , where  $\gamma(\sigma)_{ij} = (-1)^{j-i} \epsilon_{(a_i, \dots, a_{j-1}), \mathbb{Z}/m}(\sigma)$  for  $\sigma \in S$ ,  $i < j$ . By Proposition 7.1, it induces a continuous homomorphism  $\bar{\gamma}: S/N \rightarrow \bar{\text{U}}_{n+1}(\mathbb{Z}/m)$  such that  $\bar{\gamma} \circ \lambda = \pi \circ \gamma$ , where  $\lambda: S \rightarrow S/N$  and  $\pi: \text{U}_{n+1}(\mathbb{Z}/m) \rightarrow \bar{\text{U}}_{n+1}(\mathbb{Z}/m)$  are the natural epimorphisms.

Let  $(c_{ij})$  and  $(\bar{c}_{ij})$  correspond to  $\gamma$  and  $\bar{\gamma}$ , respectively, under the bijections of Lemma 8.1 and Remark 8.2. Thus

$$c_{ij} \in C^1(S, \mathbb{Z}/m), \quad \bar{c}_{ij} \in C^1(S/N, \mathbb{Z}/m), \quad c_{ij} = \inf_S(\bar{c}_{ij}),$$

and  $(\bar{c}_{ij})$  is a defining system of size  $n$  in  $C^\bullet(S/N, \mathbb{Z}/m)$ . Furthermore,  $\bar{c}_{1n} = \partial c_{1n}$ . By construction,  $\epsilon_{(a_i), \mathbb{Z}/m} = \bar{c}_{ii}$  as elements of  $H^1(S/N)$ ,  $i = 1, 2, \dots, n$ , and  $\epsilon_{w, \mathbb{Z}/m} = (-1)^n \gamma_{1, n+1} = c_{1n}$  in  $H^1(S)$ .

Now by the definition of the transgression [NSW08, Prop. 1.6.5],  $[\widetilde{c}_{1n}] = \text{trg}[c_{1n}|_N]$ . Altogether,

$$\psi_w = \langle \epsilon_{(a_1), \mathbb{Z}/m}, \dots, \epsilon_{(a_n), \mathbb{Z}/m} \rangle = \langle \bar{c}_{11}, \dots, \bar{c}_{nn} \rangle = [\widetilde{c}_{1n}] = \text{trg}[c_{1n}|_N].$$

Therefore  $(\bar{\sigma}, \psi_w)' = c_{1n}(\sigma) = \epsilon_{w, \mathbb{Z}/m}(\sigma)$ .  $\square$

## 10. PROOF OF THEOREM B

As before, let  $S = S_A$  and  $N$  a closed normal subgroup of  $S$  with  $N \leq S_{n, \mathbb{Z}/m}$ ,  $n \geq 2$ . By Lemma 6.1,  $N \leq S_{2, \mathbb{Z}/m} = S^m[S, S]$ .

**Theorem 10.1.** (a)  $(\cdot, \cdot)'$  induces a perfect pairing

$$NS_{n+1, \mathbb{Z}/m}/S_{n+1, \mathbb{Z}/m} \times H^2(S/N)_{n-\text{Massey}} \rightarrow \mathbb{Z}/m.$$

(b) There is a natural exact sequence

$$0 \rightarrow H^2(S/N)_{n-\text{Massey}} \hookrightarrow H^2(S/N) \xrightarrow{\inf} H^2(S/(N \cap S_{n+1, \mathbb{Z}/m})).$$

*Proof.* (a) In view of Lemma 5.1(b), there is a  $\mathbb{Z}/m$ -bilinear map

$$S_{n, \mathbb{Z}/m} \times \bigoplus_{\substack{w \in A^* \\ |w|=n}} \mathbb{Z}/m \rightarrow \mathbb{Z}/m, \quad (\sigma, (\bar{r}_w)) = \sum_{|w|=n} \bar{r}_w \epsilon_{w, \mathbb{Z}/m}(\sigma)$$

with left kernel  $S_{n+1, \mathbb{Z}/m}$ . Let  $\psi_w$  be as in Lemma 8.6. We consider the diagram of bilinear maps

$$(10.1) \quad \begin{array}{ccc} S_{n, \mathbb{Z}/m}/S_{n+1, \mathbb{Z}/m} & \times & \bigoplus_{w \in A^*, |w|=n} \mathbb{Z}/m \longrightarrow \mathbb{Z}/m \\ \uparrow i & & \downarrow \psi \\ N/N^m[S, N] & \times & H^2(S/N) \xrightarrow{(\cdot, \cdot)'} \mathbb{Z}/m, \end{array}$$

where  $i$  is induced by inclusion (noting that  $N^m[S, N] \leq S_{n+1, \mathbb{Z}/m}$ , by (6.1)), and  $\psi((\bar{r}_w)_w) = \sum_w \bar{r}_w \psi_w$ . By Theorem 9.2, the diagram commutes, and by (9.1), the lower map is non-degenerate. Lemma 2.2 gives a non-degenerate bilinear map as in (a), and it remains to show that it is perfect.

When the basis  $A$  of  $S$  is finite, the  $\mathbb{Z}/m$ -modules in the upper row of (10.1) are finite. Therefore so are the  $\mathbb{Z}/m$ -modules in the bilinear map (a), so its non-degeneracy implies its perfectness.

When  $A$  is infinite we write  $S = \varprojlim S_B$ , where  $B$  ranges over all finite subsets of  $A$ , and let  $\pi_B: S \rightarrow S_B$  be the associated projection. Then

$$NS_{n+1, \mathbb{Z}/m}/S_{n+1, \mathbb{Z}/m} = \varprojlim \pi_B(N)(S_B)_{n+1, \mathbb{Z}/m}/(S_B)_{n+1, \mathbb{Z}/m}$$



and by the functoriality of the Massey product,

$$H^2(S/N)_{n-\text{Massey}} = \varinjlim H^2(S_B/\pi_B(N))_{n-\text{Massey}}.$$

We now use the perfectness in the finite basis case and Lemma 2.1.

(b) As remarked above,  $N^m[S, N] \leq N \cap S_{n+1, \mathbb{Z}/m}$  and  $N \leq S^m[S, S]$ .

We may now apply Proposition 9.1 for

$$G = S, \quad T = N, \quad T_0 = N \cap S_{n+1, \mathbb{Z}/m}, \quad H = H^2(S/N)_{n-\text{Massey}}$$

and use (a). Note that  $H^2(S) = 0$ .  $\square$

Taking here  $N = S_{n, \mathbb{Z}/m}$  and  $m = p$  prime, we get Theorem B. See also [Koc02, §7.8] and [NSW08, Prop. 3.9.13] for related facts in the case  $n = 2$ .

From Theorem 10.1(a) we deduce:

**Corollary 10.2.** *Let  $N, M$  be normal closed subgroups of  $S$  with  $N \leq M \leq S_{n, \mathbb{Z}/m}$ . The following conditions are equivalent:*

- (a)  $\inf: H^2(S/M)_{n-\text{Massey}} \rightarrow H^2(S/N)_{n-\text{Massey}}$  is an isomorphism;
- (b)  $M \leq NS_{n+1, \mathbb{Z}/m}$ .

From now on we assume that  $m = p$  is prime. Recall that  $S_n = S_{n, \mathbb{Z}/p}$  (Proposition 6.2).

**Theorem 10.3.** (a)  $(\cdot, \cdot)'$  induces a non-degenerate bilinear map

$$S_n/NS_{n+1} \times \text{Ker}(H^2(S/S_n)_{n-\text{Massey}} \xrightarrow{\inf} H^2(S/N)) \rightarrow \mathbb{Z}/p.$$

(b) The kernels of the following inflation maps coincide:

$$H^2(S/S_n) \rightarrow H^2(S/NS_{n+1}), \quad H^2(S/S_n)_{n-\text{Massey}} \rightarrow H^2(S/N).$$

*Proof.* (a) Theorem 10.1(a) gives a commutative diagram of perfect pairings

$$\begin{array}{ccc} S_n/S_{n+1} & \times & H^2(S/S_n)_{n-\text{Massey}} \longrightarrow \mathbb{Z}/p \\ \uparrow & & \downarrow \inf \\ NS_{n+1}/S_{n+1} & \times & H^2(S/N)_{n-\text{Massey}} \longrightarrow \mathbb{Z}/p. \end{array} \quad \begin{array}{c} \parallel \\ \parallel \end{array}$$

Since every  $\mathbb{F}_p$ -linear space is semi-simple, we may now apply Lemma 2.3.

(b) This follows from (a) and Proposition 9.1 with

$$G = S/N, \quad T = S_n/N, \quad T_0 = NS_{n+1}/N, \quad H = H^2(S/S_n)_{n-\text{Massey}}. \quad \square$$

Now let  $G$  be a profinite group and  $\bar{G} = G(p)$  its maximal pro- $p$  quotient. Suppose that  $\bar{G} = S/N$  for a free profinite group  $S$  and a closed normal subgroup  $N$  of  $S$  with  $N \leq S_n$ ,  $n \geq 2$ .

**Corollary 10.4.** (a)  $(\cdot, \cdot)'$  induces a non-degenerate bilinear map

$$G_n/G_{n+1} \times \text{Ker}(H^2(G/G_n)_{n-\text{Massey}} \xrightarrow{\inf} H^2(G)) \rightarrow \mathbb{Z}/p.$$

(b) The kernels of the following inflation maps coincide:

$$H^2(G/G_n) \rightarrow H^2(G/G_{n+1}), \quad H^2(G/G_n)_{n-\text{Massey}} \rightarrow H^2(G).$$

*Proof.* The 5-term sequence of lower cohomologies implies that  $\inf: H^2(\bar{G}) \rightarrow H^2(G)$  is injective. Since  $G/G_k$  has a finite  $p$ -power exponent,  $G/G_k \cong \bar{G}/\bar{G}_k$  and  $G_k/G_{k+1} \cong \bar{G}_k/\bar{G}_{k+1}$  canonically for every  $k$ . Therefore we may replace  $G$  by  $\bar{G}$  to assume that  $G = S/N$ . Let  $\lambda: S \rightarrow G$  be the projection map. Then  $\lambda(S_k) = G_k$  for every  $k$ . Moreover,  $S/S_n \cong G/G_n$  and  $S_n/NS_{n+1} \cong G_n/G_{n+1}$ . We now apply Theorem 10.3.  $\square$

See [Bog92, Lemma 3.3] in the case  $n = 2$ . Corollary 10.2 gives, by a similar reduction to the maximal pro- $p$  quotient:

**Corollary 10.5.** *Let  $\bar{M}$  be a normal subgroup of  $G$  contained in  $G_n$ . Then  $\inf: H^2(G/\bar{M})_{n-\text{Massey}} \rightarrow H^2(G)_{n-\text{Massey}}$  is an isomorphism if and only if  $\bar{M} \leq G_{n+1}$ . In particular,  $H^2(G/G_{n+1})_{n-\text{Massey}} \cong H^2(G)_{n-\text{Massey}}$ .*

For  $n = 2$  this was proved in [EM11b, Cor. 5.2, Th. A], extending earlier results from [CEM12].

## 11. PROOF OF THEOREM A'

Let again  $S = S_A$ ,  $m = p$  prime, and  $N$  a normal subgroup of  $S$  contained in  $S_n$ . The following theorem is an equivalent form of Theorem A' when we take  $G = S/N$ . We note that while  $H^2(S/S_n)_{n-\text{Massey}}$  is generated by (elementary)  $n$ -fold Massey products, this property need not be inherited by its subgroups.

**Theorem 11.1.** *Let  $n \geq 1$ . When  $n \geq 2$  we assume that*

$$\text{Ker}(H^2(S/S_n)_{n-\text{Massey}} \xrightarrow{\inf} H^2(S/N))$$

*is generated by  $n$ -fold Massey products. Then  $NS_{n+1} = \bigcap M$ , where  $M$  ranges over all open normal subgroups of  $S$  containing  $N$  such that  $S/M$  embeds as a subgroup of  $U_{n+1}(\mathbb{Z}/p)$ .*

*Proof.* We argue by induction on  $n$ . For  $n = 1$  we have by Lemma 6.1,  $S_2 = S^p[S, S]$ , so  $S/NS_2$  is an elementary abelian  $p$ -group. Consequently,  $NS_2 = \bigcap M$ , where  $M$  ranges over all open normal subgroups of  $S$  containing  $N$  such that  $S/M \cong \mathbb{Z}/p \cong U_2(\mathbb{Z}/p)$ .

Let  $n \geq 2$ . We assume the assertion for  $n - 1$  and prove it for  $n$ .

When  $n \geq 3$  Theorem 10.1(b) implies that

$$\inf: H^2(S/S_{n-1})_{(n-1)\text{-Massey}} \rightarrow H^2(S/S_n)$$

is the zero map, so trivially, its kernel is generated by  $(n-1)$ -fold Massey products. We may therefore apply the induction hypothesis for  $n-1$  and  $N = S_n$  (also when  $n=2$ ), to get  $S_n = \bigcap M$ , where  $M$  ranges over all open normal subgroups of  $S$  containing  $S_n$  such that  $S/M$  embeds as subgroup of  $U_n(\mathbb{Z}/p)$ .

Next, we have already noted in the proof of Theorem 10.3(b) that (a) and (b) of Proposition 9.1 hold with  $G = S/N$ ,  $T = S_n/N$ ,  $T_0 = NS_{n+1}/N$ ,  $H = H^2(S/S_n)_{n\text{-Massey}}$ . By assumption, the set  $H_0$  of all  $n$ -fold Massey products in  $\text{Ker}(\inf: H \rightarrow H^2(G))$  generates this kernel. Therefore (c) of Proposition 9.1 also holds in this setup.

By Proposition 8.3, the central extensions corresponding to  $n$ -fold Massey products in  $H$  are (up to signs) as in the lower part of the diagram

$$\begin{array}{ccccccc} & & & & G & & \\ & & & \swarrow \hat{\Phi} & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}/p & \longrightarrow & U_{n+1}(\mathbb{Z}/p) \times_{\bar{U}_{n+1}(\mathbb{Z}/p)} (S/S_n) & \xrightarrow{\text{pr}_2} & S/S_n \longrightarrow 1, \end{array}$$

where the fiber product is with respect to the projection  $\pi: U_{n+1}(\mathbb{Z}/p) \rightarrow \bar{U}_{n+1}(\mathbb{Z}/p)$  and some continuous homomorphism  $\bar{\gamma}: S/S_n \rightarrow \bar{U}_{n+1}(\mathbb{Z}/p)$ . The corresponding Massey product is in the kernel of  $\inf: H^2(S/S_n) \rightarrow H^2(G)$  (i.e., belongs to  $H_0$ ) if and only if there is a continuous homomorphism  $\hat{\Phi}$  making the diagram commutative [Hoe68, 1.1]. We therefore conclude from (c) of Proposition 9.1 that

$$NS_{n+1}/N = \bigcap \text{Ker}(\hat{\Phi}),$$

where  $\hat{\Phi}$  ranges over all continuous homomorphisms making the diagram commutative for some  $\bar{\gamma}$ . By Lemma 7.3, the subgroups  $\text{Ker}(\hat{\Phi})$  are exactly the quotients  $(M \cap S_n)/N$ , where  $M$  is a normal open subgroup of  $S$  containing  $N$  such that  $S/M$  embeds in  $U_{n+1}(\mathbb{Z}/p)$ . Hence,  $NS_{n+1} = (\bigcap M) \cap S_n$ . Since  $U_n(\mathbb{Z}/p)$  embeds as a subgroup of  $U_{n+1}(\mathbb{Z}/p)$ , and by what we have seen earlier in the proof,  $S_n$  contains  $\bigcap M$ , so in fact  $NS_{n+1} = \bigcap M$ .  $\square$

**Remark 11.2.** In our general setup, the projection  $S \rightarrow G$  induces an isomorphism  $S/S_n \cong G/G_n$ . When it further induces an isomorphism  $S/S_{n+1} \cong G/G_{n+1}$ , i.e.,  $N \leq S_{n+1}$ , Theorem 10.1(b) shows that the assumption about the kernel in Theorem 11.1 is satisfied. This example is not exhaustive (see Corollary 12.3).

**Remark 11.3.** As in Corollary 10.4, we may replace in Theorem A' the group  $G$  by its maximal pro- $p$  quotient  $G(p)$  to assume that  $G(p)$  (but not necessarily  $G$ ) has a presentation  $S/N$  with  $N \leq S_n$ .

**Corollary 11.4.** *Let  $G$  be a profinite group with  $\text{cd}_p(G) \leq 1$ . Then  $G_n = \bigcap_{\rho} \text{Ker}(\rho)$ , where  $\rho$  ranges over all representations of  $G$  in  $U_n(\mathbb{F}_p)$ .*

*Proof.* The maximal pro- $p$  quotient  $G(p)$  of  $G$  is a free pro- $p$  group [NSW08, Prop. 3.5.3 and Prop. 3.5.9]. We may therefore replace  $G$  by  $G(p)$ , to assume that  $G$  is a free pro- $p$  group.

As  $H^2(G) = 0$ , all Massey kernel conditions are satisfied. Take a free profinite group  $S$  on the same basis as  $G$  and let  $N = \text{Ker}(S \rightarrow S(p) = G)$ . Since  $S/S_n$  has a  $p$ -power exponent,  $N \leq S_n$  for every  $n$ . Now apply Theorem A'.  $\square$

## 12. EXAMPLES

We conclude by examining Theorem A' in low degrees.

**Example 12.1.** When  $n = 1$  Theorem A' is just the elementary fact that  $G^p[G, G] = \bigcap M$ , where  $M$  ranges over all open normal subgroups of  $G$  with  $G/M \cong \{1\}, \mathbb{Z}/p$ .

**Example 12.2.** Let  $n = 2$ . Assume that the kernel of  $\inf: H^2(S/S_2)_{2\text{-Massey}} = H^2(G/S_2)_{\text{dec}} \rightarrow H^2(G)$  is generated by cup products (see Example 8.5).

When  $p = 2$ ,  $U_3(\mathbb{Z}/2)$  is the dihedral group  $D_4$  of order 8. Hence in this case Theorem A' asserts that

$$(12.1) \quad G_3 = \bigcap \left\{ \bar{M} \mid \bar{M} \trianglelefteq G, G/\bar{M} \cong \{1\}, \mathbb{Z}/2, \mathbb{Z}/4, D_4 \right\}.$$

This recovers [EM11a, Cor. 11.3], which in turn generalizes [MSp96, Cor. 2.18] (see below).

When  $p > 2$ ,  $U_3(\mathbb{Z}/p)$  is the unique nonabelian group  $H_{p^3}$  of order  $p^3$  and exponent  $p$  (also called the *Heisenberg group*). Its subgroups are  $\{1\}$ ,  $\mathbb{Z}/p$ ,  $(\mathbb{Z}/p)^2$  and  $U_3(\mathbb{Z}/p)$  itself. Moreover, when  $G/\bar{M} \cong (\mathbb{Z}/p)^2$ , we may write  $\bar{M} = \bar{M}_1 \cap \bar{M}_2$  with  $G/\bar{M}_i \cong \mathbb{Z}/p$ ,  $i = 1, 2$ . Therefore

$$(12.2) \quad G_3 = \bigcap \left\{ \bar{M} \mid \bar{M} \trianglelefteq G, G/\bar{M} \cong \{1\}, \mathbb{Z}/p, H_{p^3} \right\}.$$

This recovers [EM11b, Example 9.5(1)].

Finally we recover [MSp96, Cor. 2.18] and [EM11b, Th. D] (see also [NQD12]):

**Corollary 12.3.** *Let  $K$  be a field containing a root of unity of order  $p$  and  $G = G_K$  its absolute Galois group. Then  $G_3 = \bigcap \bar{M}$ , where  $\bar{M}$  ranges over all open normal subgroups of  $G$  such that  $G/\bar{M}$  embeds in  $U_3(\mathbb{Z}/p)$ .*

*Proof.* The injectivity of the Galois symbol in degree 2, which is a part of the Merkurjev–Suslin theorem ([MS82], [GS06]), implies that the kernel of  $\inf: H^2(S/S^p[S, S])_{\text{dec}} = H^2(G/G^p[G, G])_{\text{dec}} \rightarrow H^2(G)$  is generated by cup products (see [Bog91], [EM11a, Prop. 3.2]). Now apply Theorem A'.  $\square$

## REFERENCES

- [Bog91] F. A. Bogomolov, *On two conjectures in birational algebraic geometry*, Proc. of Tokyo Satellite conference ICM-90 Analytic and Algebraic Geometry, 1991, pp. 26–52.
- [Bog92] F. A. Bogomolov, *Abelian subgroups of Galois groups*, Math. USSR, Izv. **38** (1992), 27–67 (English; Russian original).
- [CEM12] S. K. Chebolu, I. Efrat, and J. Mináč, *Quotients of absolute Galois groups which determine the entire Galois cohomology*, Math. Ann. **352** (2012), 205–221.
- [DDMS] J. D. Dixon, M. du Sautoy, A. Mann, and D. Segal, *Analytic Pro- $p$  Groups*, Cambridge Stud. Adv. Math., vol. 61, Cambridge University Press, 1999.
- [Dwy75] W. G. Dwyer, *Homology, Massey products and maps between groups*, J. Pure Appl. Algebra **6** (1975), 177–190.
- [Efr12] I. Efrat, *Uniqueness of Massey products* (2012), to appear.
- [EM11a] I. Efrat and J. Mináč, *On the descending central sequence of absolute Galois groups*, Amer. J. Math. **133** (2011), 1503–1532.
- [EM11b] I. Efrat and J. Mináč, *Galois groups and cohomological functors* (2011), to appear, available at [arXiv:1103.1508v1](https://arxiv.org/abs/1103.1508).
- [Fen83] R. A. Fenn, *Techniques of Geometric Topology*, London Math. Society Lect. Note Series, vol. 57, Cambridge Univ. Press, Cambridge, 1983.
- [FS84] R. Fenn and D. Sjerve, *Basic commutators and minimal Massey products*, Canad. J. Math. **36** (1984), 1119–1146.
- [FJ08] M. D. Fried and M. Jarden, *Field arithmetic*, 3rd ed., Springer, Berlin, 2008.
- [Gär12] J. Gärtner, *Higher Massey products in the cohomology of mild pro- $p$ -groups* (2012), preprint, available at [arXiv:1212.2118](https://arxiv.org/abs/1212.2118).
- [GLMS03] W. Gao, D. B. Leep, J. Mináč, and T. L. Smith, *Galois groups over nonrigid fields*, Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999), Fields Inst. Commun., vol. 33, Amer. Math. Soc., Providence, RI, 2003, pp. 61–77.
- [GS06] P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press, Cambridge, 2006.
- [Hoe68] K. Hoechsmann, *Zum Einbettungsproblem*, J. reine angew. Math. **229** (1968), 81–106.
- [HW12] M. Hopkins and K. Wickelgren, *Splitting varieties for triple Massey products* (2012), preprint, available at [arXiv:1210.4964](https://arxiv.org/abs/1210.4964).

- [Jen41] S. A. Jennings, *The structure of the group ring of a  $p$ -group over a modular field*, Trans. Amer. Math. Soc. **50** (1941), 175–185.
- [Koc02] H. Koch, *Galois Theory of  $p$ -Extensions*, Springer, Berlin, 2002.
- [Kra66] D. Kraines, *Massey higher products*, Trans. Amer. Math. Soc. **124** (1966), 431–449.
- [Lab06] J. Labute, *Mild pro- $p$ -groups and Galois groups of  $p$ -extensions of  $\mathbb{Q}$* , J. reine angew. Math. **596** (2006), 155–182.
- [LM11] J. Labute and J. Mináč, *Mild pro-2-groups and 2-extensions of  $\mathbb{Q}$  with restricted ramification*, J. Algebra **332** (2011), 136–158.
- [Laz65] M. Lazard, *Groupes analytiques  $p$ -adiques*, Inst. Hautes Études Sci. Publ. Math. **26** (1965), 389–603.
- [May69] J. P. May, *Matric Massey products*, J. Algebra **12** (1969), 533–568.
- [MS82] A. S. Merkurjev and A. A. Suslin,  *$K$ -cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), 1011–1046 (Russian); English transl., Math. USSR Izv. **21** (1983), 307–340.
- [MSp96] J. Mináč and M. Spira, *Witt rings and Galois groups*, Ann. Math. **144** (1996), 35–60.
- [Mor04] M. Morishita, *Milnor invariants and Massey products for prime numbers*, Compositio Math. **140** (2004), 69–83.
- [Mor12] M. Morishita, *Knots and primes*, Universitext, Springer, London, 2012.
- [NSW08] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields, Second edition*, Springer, Berlin, 2008.
- [NQD12] T. Nguyen Quang Do, *Étude Kummerienne de la  $q$ -suite centrale descendante d'un group de Galois*, Publ. Math. Besançon Algèbre Théorie Nr., vol. 2012/2, Presses Univ. Franche-Comté, Besançon, 2012, pp. 121–137.
- [RZ10] L. Ribes and P. Zalesskii, *Profinite Groups*, Springer, 2010.
- [Sha07] R. T. Sharifi, *Massey products and ideal class groups*, J. reine angew. Math. **603** (2007), 1–33.
- [Sta65] J. Stallings, *Homology and central series of groups*, J. Algebra **2** (1965), 170–181.
- [Vog05] D. Vogel, *On the Galois group of 2-extensions with restricted ramification*, J. reine angew. Math. **581** (2005), 117–150.
- [Wic09] K. Wickelgren, *Lower central series obstructions to homotopy sections of curves over number fields*, Ph.D. Thesis, Stanford University, 2009.
- [Wic12] K. Wickelgren,  *$n$ -Nilpotent obstructions to  $\pi_1$ -sections of  $\mathbb{P}^1 \setminus \{0, 1, \infty\}$  and Massey products*, Conference on Galois-Teichmüller Theory and Arithmetic Geometry (H. Nakamura et al, eds.) (Kyoto, 2010), Advanced studies in pure mathematics, vol. 63, Mathematical Society of Japan, 2012, pp. 579–600.
- [Zas39] H. Zassenhaus, *Ein Verfahren, jeder endlichen  $p$ -Gruppe einen Lie-Ring mit der Charakteristik  $p$  zuzuordnen*, Abh. Math. Semin. Univ. Hamburg **13** (1939), 200–207.

MATHEMATICS DEPARTMENT, BEN-GURION UNIVERSITY OF THE NEGEV, P.O.  
BOX 653, BE'ER-SHEVA 84105, ISRAEL  
*E-mail address:* efrat@math.bgu.ac.il